UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,487	02/02/2001	Gregg B. Morrison	145415.00001	5305

27781 7590 06/17/2004

POWELL, GOLDSTEIN, FRAZER & MURPHY LLP
P.O. BOX 97233
WASHINGTON, DC 20090-7223

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	7

DATE MAILED: 06/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/773,487	MORRISON, GREGG B.	
	Examiner	Art Unit	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-66* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-66* is/are rejected.

7)☒ Claim(s) *50-53* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-66 have been examined.

Claim Objections

2. Claims 50-53 are objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-4, 15-21, and 23-25 are rejected under 35 U.S.C. 102(b) as being anticipated by Baena-Arnaiz et al. (hereinafter refereed to as Baena) (US Patent No. 6,006,190).

5. As per claim 1, Baena teaches a process for securing information in a digital form comprising:

creating an identifier using information obtained from a device capable of rendering the digitized information to be secured [column 4, lines 37-57];

associating the identifier with the information to be rendered [column 4, lines 54-57 and column 2, lines 42-46];

securing said digitized information by preventing the rendering of the information if the identity of the device upon which the information is to be rendered is not verified using said identifier [column 1, lines 36-42 and column 7, lines 33-35].

6. As per claim 15, Baena teaches a process for securely transferring information in a digital form comprising:

obtaining information to be distributed, wherein the information is in a digital form (i.e. software) [column 3, lines 28-31 and column 6, lines 52-59];

producing a binary key of at least 64 bits using information associated with the device that is to render the information after it has been distributed [column 4, lines 37-43];

encoding the information by using the unique identifier in combination with an algorithm suitable for encoding such information [column 4, lines 37-57];

transferring the information to the location at which the device that is to render the information is located [column 6, lines 52-55];

decoding the information by producing a binary key by collecting information from the device that is to render the information after receiving the information [column 7, lines 18-22] ;

decoding the encoded information using the binary key [column 7, lines 18-22].

7. As per claims 23, Baena teaches a process of installing software in a manner that prevents the unauthorized duplication or use of the software after it has been installed on a specific computer, wherein the process comprises:

during the process of installation of the software onto the computer:

producing a unique identifier using information derived from the physical components of the workstation onto which the software is to be installed [column 4, lines 37-57];

including the unique identifier into one or more of the files associated with the software as installed [column 4, lines 54-57 and column 2, lines 42-46];

at the time of initiation of execution of the software by a user after it has been installed,

producing a unique identifier using information derived from the physical components of the workstation onto which the software is to be installed [column 7, lines 1-4];

comparing the unique identifier with a unique identifier included in one or more of the files associated with the software to executed [column 7, lines 32-35]; and

if the comparison provides a pre-defined negative result based on the unique identifiers, preventing the software from executing [column 7, lines 32-35 and column 8, lines 2-25].

8. As per claim 24, Baena teaches a process for preventing the installation or operation of software other than from a specified physical medium comprising:

prior to encoding data onto a computer-readable medium wherein the data comprises files used to install the software, producing a unique identifier using information associated with the physical structure of the medium [column 4, lines 37-57];

including the unique identifier in one or more files used in the installation process for the said software [column 4, lines 54-57 and column 2, lines 42-46];

during the process of installation of the software, producing a unique identifier using information derived from the physical structure of the medium [column 7, lines 1-5];

comparing the unique identifier to the unique identifier included in the at least one file used in the installation process for the said software [column 7, lines 33-36];

if the comparison provides a pre-defined negative result based on the unique identifiers, causing the termination of the installation process [column 7, lines 33-36 and column 8, lines 2-25].

9. As per claim 2, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the identifier is a binary key suitable for use in an algorithm that can secure said digitized information [column 4, lines, 30-32 and lines 38-40].

10. As per claims 3 and 4, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the identifier is produced by evaluating information associated with a specific physical device that can render the secured information and the identifier uniquely identifies said device [column 4, lines 42-57].

11. As per claim 16, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the steps of decoding the encoded information are performed incidental to the process of rendering the information (i.e. during execution of the information) [column 7, lines 36-37].

12. As per claim 17, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the device used in rendering the information produces the key incidental to the process of decoding and rendering the encoded information [column 7, lines 1-2 and 36-37].

13. As per claim 18, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the encoded information are performed by a distinct device from the device that renders the information [column 2, lines 37-47].

14. As per claim 19, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the steps of decoding the encoded information are performed by the device that renders the information [column 7, lines 1-4].

15. As per claim 20, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the key is associated with the data containing the encoded information [column 4, lines 54-57 and column 2, lines 42-46].

16. As per claim 21, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the key is transferred distinct from the file containing the encoded information [column 6, lines 52-55];

17. As per claim 25, Baena teaches the process as applied above. Furthermore, Baena teaches the process wherein the information is secured by preventing the reading of data from the medium containing the software to be installed [column 2, lines 48-55].

18. Claim 54 is rejected under 35 U.S.C. 102(b) as being anticipated by Kupka et al. (hereinafter refereed to as Kupka) (PCT WO/99/55055).

19. As per claim 54, Kupka teaches process of preventing the unauthorized rendering of information originally stored on an optically readable medium, wherein the process comprises:

defining a unique identifier for the information to be secured and incorporating a unique physical media identifier into the physical structure of the optically readable medium [page 16, 13-20 and page 4, lines 21-29];

producing a binary key of at least 128 bits using the unique identifier for the information to be secured and the physical media identifier [page 17, lines 24-29];

encoding the binary key on the optical medium in a form readable by a device that can render the information [page 4, lines 21-29];

prior to or during the rendering of the information by the device causing the device to evaluate the physical media to detect the binary key and the unique physical media identifier [page 5, lines 12-30];

evaluating the information obtained by the detection step to determine if the information to be rendered is encoded on the optical medium having the unique physical media identifier and if the evaluation step provides a pre-defined negative result, preventing the device from rendering the encoded information [page 5, lines 17-24 and page 6 lines 27-32].

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 5-14, 22, 26-29, 43-53 and 63-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baena-Arnaiz (US Patent No. 6,006,190).

22. As per claims 43 and 63, Baena teaches a process for securely distributing information representing an audio or audiovisual work comprising:

producing a binary key using information derived from at least one physical component of a device capable of rendering the work [column 4, lines 37-57];

distributing the information to the location at which the information is to be rendered [column 6, lines 52-55];

prior to or during the rendering of the information on a device capable of rendering said information, producing a binary key using information derived from at least one physical component of the device [column 7, lines 1-5 and column 4, lines 37-57];

retrieving from said information the binary key associated with said information and comparing the binary key extracted from said information with the binary key produced using information from the device [column 7, lines 33-36];

preventing the rendering of the information if the binary key associated with the information is not identical to the binary key produced using the device [column 7, lines 33-36 and column 8, lines 2-25].

Furthermore, Baena teaches associating the information representing software work with the binary key produced [column 4, lines 54-57 and column 2, lines 42-46]. However Baena does not explicitly teach associating with the information representing the audio or audiovisual work the binary key produced. It would have been obvious to one having ordinary skill in the art at the time the invention was made to associate with the information representing the audio or audiovisual work the binary key produced. It would have been obvious because Baena teaches

associating the information representing software work with the binary key produced column 4, lines 54-57 and column 2, lines 42-46].

23. As per claims 5 and 22, Baena teaches the process as applied to claim 2 and 15 above. Furthermore, Baena teaches obtaining information representing a physical or functional attribute of at least one component in said physical device which is unique to that component [column 4, lines 37-57]; and converting said information into binary key [column 4, line 37]. However Baena does not explicitly teach performing a cyclic redundancy check on the information. It would have been obvious to one having ordinary skill in the art at the time the invention was made to perform cyclic redundancy check on the information in order to convert it to binary key. It would have been obvious because Baena teaches generating 64 bit unique binary key [column 4, lines 36-38].

24. As per claim 6, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the identifier comprises a binary key of at least 64 bits in length [column 4, lines 27].

25. As per claims 7-14, Baena teaches the process as applied above. Furthermore, Baena teaches generating the key using information unique to the device, and encrypting data using the generated key and preventing rendering of data when the key used for encryption is not associated with the device [column 4, lines 37-57 and column 7, lines 33-35].

26. As per claims 26-29, Baena teaches the process as applied above. Beana does not explicitly teach intentionally altering the physical structure of a device. However it is well known

in the art to intentionally alter physical structure of a device in order to incorporate a pre-defined arbitrary identifier.

27. As per claims 44 and 45, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the device is selected from the group consisting of a general purpose computer, a special purpose computer, a DVD player, a CD player, a motion picture projector or a device that comprises a video display unit in combination with circuitry capable of rendering an audiovisual work in a digital form [column 2, lines 23-30].

28. As per claims 46-49, Baena teaches the process as applied above. Furthermore, Baena teaches producing a binary key using attributes of a device and associating the key with the information distributing medium or the information [column 4, lines 54-57 and column 2, lines 42-46].

29. As per claims 50-53, Baena teaches the process as applied to claim 43 above. Furthermore, Baena teaches preventing the rendering of the information if the binary key associated with the information is not identical to the binary key produced using the device [column 7, lines 33-36 and column 8, lines 2-25].

30. As per claim 64, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the steps of decoding the encoded information are performed contemporaneously with the process of rendering the information (i.e. during execution of the information) [column 7, lines 36-37].

31. As per claims 65 and 66, Baena teaches the process as applied above. Furthermore, Baena teaches the process, wherein the unique keys specific to the device [column 4, lines 42-57].

32. Claims 55-62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kupka (PCT WO 99/55055).

As per claims 55-62, Kupka teaches the process as applied to claim 54 above. Furthermore, Kupka teaches defining a unique identifier for the information to be secured and incorporating a unique physical media identifier into the physical structure of the optically readable medium [page 16, 13-20 and page 4, lines 21-29]. However Kupka does not explicitly teach physically altering a portion of the optical medium. However it is well known in the art to intentionally alter physical structure of a device in order to incorporate a pre-defined arbitrary identifier.

33. Claims 30-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Baena-Arnaiz (US Patent No. 6,006,190) in view of Kupka et al. (hereinafter refereed to as Kupka) (PCT WO 99/55055).

34. As per claim 30, Baena teaches a process of installing software across in a manner that prevents the unauthorized duplication or use of the software after it has been installed on a specific computer comprising:

initiating an installation process for installing software onto a computer [column 6, lines 54-58];

producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed [column 4, lines 37-57];

including the unique identifier in at least one file associated with the software to be installed, wherein the absence of said file prevents operation of the software [column 4, lines 54-57 and column 2, lines 42-46];

transferring the files including at least the said file containing the included identifier to the computer upon which the software is to be installed [column 6, lines 52-55];

at the time of execution of the software after it has been installed, producing a unique identifier using information derived from at least one physical component of the computer upon which the software is to be installed [column 7, lines 1-5 and column 4, lines 37-57];

comparing the unique identifier to the unique identifier embedded in the said at least one file associated with the software and if the comparison provides a pre-defined negative result based on the unique identifiers, preventing the software from executing, preventing the operation of the software [column 7, lines 33-36 and column 8, lines 2-25].

Baena does not explicitly teach installing software from a server on to a computer using a network. However, Kupka teaches installing software from a server onto a device using a network [page 4, lines 12-20 and figure 1]. It would have been obvious to one having ordinary skill in the art at the time the invention was made to install software from a server onto a device using a network as per teachings of Kupka into the software installation system taught by Baena in order to have a faster and wider distribution means.

35. As per claim 31, the combination of Baena and Kupka teaches the process as applied above. Furthermore, Kupka teaches generating unique device identifier at the server [page 4, lines 21-29].

36. As per claims 33-36, the combination of Baena and Kupka teaches the prcess as applied above. Furthermore, Baena teaches generating hardware specific key [column 4, lines 47-54].

37. As per claims 32 and 37-42, the combination of Baena and Kupka teaches the processas applied above. Furthermore, Kupka teaches using the unique device identifier and other information to encrypt data [page 19, lines 29-31].

Conclusion

38. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Beemnet Dada

June 10, 2004